AMENDMENTS TO CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A data carrier ~~with~~ comprising:

a semiconductor chip ~~(5)~~ having:

at least one memory;

~~in which~~ an operating program stored in said memory; and

~~containing~~ a plurality of operating program commands ~~is stored~~ contained in said operating program, each command causing signals detectable from outside the semiconductor chip (5) during execution of the command within the semiconductor chip, ~~characterized in that~~

wherein the data carrier ~~(1)~~ is ~~designed~~ arranged to perform security-relevant operations solely by executing selected said operating program commands under one of the following conditions:

said selected operating program commands are of such a kind that data processed with the corresponding commands cannot be inferred from detected signals that have been detected outside the semiconductor chip, or ~~executing~~

said operating program commands are executed by the data carrier in such a way[[,]] that the data processed with the corresponding commands cannot be inferred from the detected signals.

2. (Currently Amended) A data carrier according to claim 1, ~~characterized in that~~ wherein the executed operating program commands ~~used~~ are designed for at least byte-by-byte processing of data.

3. (Currently Amended) A data carrier according to claim 1, ~~characterized in that~~ wherein the operating program commands ~~used~~ are ~~indistinguishable with respect to the~~ selected such that the commands cannot be distinguished based on signal patterns caused thereby.

4. (Currently Amended) A data carrier according to claim 1, ~~characterized in that~~ wherein the executed operating program commands ~~used~~ each lead to a signal pattern which is substantially independent of the data processed with the corresponding command.

5. (Currently Amended) A data carrier according to claim 1, ~~characterized in that~~ wherein the operating program is ~~able~~ arranged to execute a series of operations (*f*), input data being required for executing the operations (*f*) and output data being generated by execution of the operations (*f*), ~~whereby~~ said operations (*f*) including the following operations:

- falsification the input data ~~are falsified~~ by combination with auxiliary data (*Z*) before execution of one or more operations (*f*),
- combination of the output data determined by execution of the one or more operations (*f*) ~~are combined~~ with an auxiliary function value (*f*(*Z*)) in order to compensate for the falsification of the input data,
- ~~whereby~~ wherein the auxiliary function value (*f*(*Z*)) was previously determined by execution of the one or more operations (*f*) with the auxiliary data (*Z*) as input data in safe surroundings and stored on the data carrier (1) along with the auxiliary data (*Z*).

6. (Currently Amended) A data carrier according to claim 5, ~~characterized in that~~ wherein the combination with the auxiliary function values (*f*(*Z*)) for compensating the falsification is performed at the latest directly before execution of an operation (*g*) which is nonlinear with respect to the combination generating the falsification.

7. (Currently Amended) A data carrier according to claim 5, ~~characterized in that~~ wherein the auxiliary data (*Z*) are varied, the corresponding function values being stored in the memory of the data carrier~~(1)~~.

8. (Currently Amended) A data carrier according to claim 7, ~~characterized in that~~ wherein new auxiliary values (*Z*) and new auxiliary function values (*f*(*Z*)) are generated by combining two or more existing auxiliary data (*Z*) and auxiliary function values (*f*(*Z*)).

9. (Currently Amended) A data carrier according to claim 8, ~~characterized in that~~ wherein the two or more existing auxiliary data (*Z*) and auxiliary function values (*f*(*Z*)) intended for the combination are each selected randomly.

10. (Currently Amended) A data carrier according to claim 5, ~~characterized in that~~ wherein pairs of auxiliary data (*Z*) and auxiliary function values (*f*(*Z*)) are generated by a generator without the operation (*f*(*Z*)) being applied to the auxiliary data (*Z*).

11. (Currently Amended) A data carrier according to claim 5, ~~characterized in that~~ wherein the auxiliary data (*Z*) are a random number.

12. (Currently Amended) A data carrier according to claim 5, ~~characterized in that~~ wherein the combination is an ~~EXOR~~ XOR operation.

13. (Currently Amended) A data carrier according to claim 1, ~~characterized in that~~ wherein the operating program is arranged to execute a plurality of operations ~~can be executed with the operating program, it holding~~, wherein for at least a subset of said operations, ~~that~~ the total result achieved by execution of several operations of the subset does not depend on the order of execution of the operations, and wherein the order of execution of the stated subset of operations is varied at least when the subset contains one or more security-relevant operations.

14. (Currently Amended) A data carrier according to claim 13, ~~characterized in that~~ wherein the order of execution is varied at each run through the stated subset of operations.

15. (Currently Amended) A data carrier according to claim 13, ~~characterized in that~~ wherein the order of execution is varied according to a fixed principle.

16. (Currently Amended) A data carrier according to claim 13, ~~characterized in that~~ wherein the order of execution is varied randomly.

17. (Currently Amended) A data carrier according to claim 13, ~~characterized in that~~ wherein the order of execution is varied in accordance with the data processed with the operations (*f*).

18. (Currently Amended) A data carrier according to claim 13, ~~characterized in that~~ wherein the order of execution is fixed before execution of the first operation (*f*) of the subset for all operation of the subset whose execution is intended to be directly successive.

19. (Currently Amended) A data carrier according to claim 13, ~~characterized in that it is fixed~~ wherein, before the onset of execution of an operation (*f*) of the subset, ~~which~~ the operation of the subset whose execution is intended to be successive and that is to be executed next, is ~~executed next~~ fixed.

20. (Currently Amended) A data carrier according to claim 1, ~~characterized in that~~ wherein the security-relevant operations are key permutations or permutations of other secret data.

21. (Currently Amended) A data carrier according to claim 1, ~~characterized in that~~ wherein the data carrier is a smart card.

22. (Currently Amended) A method for executing security-relevant operations in a data carrier ~~(1)~~ with a semiconductor chip ~~(5)~~ having at least one memory in which an operating program containing a plurality of commands is stored, each command causing signals detectable from outside the semiconductor chip ~~(5)~~ during execution of the command within the semiconductor chip, ~~characterized in that~~ comprising the step of causing the data carrier to perform security-

relevant operations (*f*) solely ~~using~~ by executing said operating program commands, said step of causing the data carrier to perform security-relevant operations comprising one of the following steps:

executing only selected said operating program commands that are of such a kind that data processed with the corresponding commands cannot be inferred from detected signals that have been detected outside the semiconductor chip, or ~~using~~

executing said operating program commands in such a way[[,]] that the data processed with the corresponding commands cannot be inferred from the detected signals.

23. (Currently Amended) A method according to claim 22, ~~characterized in that~~ wherein the executed operating program commands ~~used~~ employ data present at least byte by byte.

24. (Currently Amended) A method according to claim 22, ~~characterized in that~~ wherein the operating program commands ~~used~~ are ~~indistinguishable with respect to the~~ selected such that the commands cannot be distinguished based on signal patterns caused thereby.

25. (Currently Amended) A method according to claim 22, ~~characterized in that~~ wherein the executed operating program commands ~~used~~ each lead to a signal pattern which is substantially independent of the data processed with the command.

26. (Currently Amended) A method for protecting secret data serving as input data for one or more operations, ~~characterized in that~~ comprising the steps of:

- falsifying the input data ~~are falsified~~ by combination with auxiliary data (*Z*) before execution of one or more operations (*f*),
- combining the output data determined by execution of the one or more operations (*f*) ~~are combined~~ with an auxiliary function value (*f*(*Z*)) in order to compensate for the falsification of the input data,

- ~~whereby~~ wherein the auxiliary function value ($f(Z)$) was previously determined by execution of the one or more operations (f) with the auxiliary data (Z) as input data in safe surroundings and stored along with the auxiliary data (Z).

27. (Currently Amended) A method according to claim 26, ~~characterized in that~~ wherein the combination with the auxiliary function values ($f(Z)$) for compensating the falsification is performed at the latest directly before execution of an operation (g) which is nonlinear with respect to the combination generating the falsification.

28. (Currently Amended) A method according to claim 26, ~~characterized in that~~ wherein the auxiliary data (Z) are varied, the corresponding function values being stored in the memory of the data carrier.

29. (Currently Amended) A method according to claim 28, ~~characterized in that~~ wherein new auxiliary values (Z) and new auxiliary function values ($f(Z)$) are generated by combining two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$).

30. (Currently Amended) A method according to claim 29, ~~characterized in that~~ wherein the two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$) intended for the combination are each selected randomly.

31. (Currently Amended) A method according to claim 26, ~~characterized in that~~ wherein pairs of auxiliary data (Z) and auxiliary function values ($f(Z)$) are generated by a generator without the operation ($f(Z)$) being applied to the auxiliary data (Z).

32. (Currently Amended) A method according to claim 26, ~~characterized in that~~ wherein the auxiliary data (Z) are a random number.

33. (Currently Amended) A method according to claim 26, ~~characterized in that~~ wherein the combination is an ~~EXOR~~ XOR operation.

34. (Currently Amended) A method for executing a plurality of operations (*f*) within the operating system of a data carrier ~~(1)~~, ~~it holding~~ comprising the steps of:

executing the plurality of operations (*f*) in such a manner that, for at least a subset of said operations, ~~that~~ the total result achieved by execution of several operations of the subset does not depend on the order of execution of the operations, and

varying the order of execution of the stated subset of operations ~~is varied~~ at least when the subset contains one or more security-relevant operations.

35. (Currently Amended) A method according to claim 34, ~~characterized in that~~ wherein the order of execution is varied at each run through the stated subset of operations.

36. (Currently Amended) A method according to claim 34, ~~characterized in that~~ wherein the order of execution is varied according to a fixed principle.

37. (Currently Amended) A method according to claim 34, ~~characterized in that~~ wherein the order of execution is varied randomly.

38. (Currently Amended) A method according to claim 34, ~~characterized in that~~ wherein the order of execution is varied in accordance with the data processed with the operations (*f*).

39. (Currently Amended) A method according to claim 34, ~~characterized in that~~ wherein the order of execution is fixed before execution of the first operation (*f*) of the subset for all operation of the subset whose execution is intended to be directly successive.

40. (Currently Amended) A method according to claim 35, ~~characterized in that it is fixed~~ further comprising the step of fixing, before the onset of execution of an operation (*f*) of the subset, which operation of the subset whose execution is intended to be successive is executed next.

41. (Currently Amended) A method according to claim 22, ~~characterized in that~~ wherein the security-relevant operations are key permutations or permutations of other secret data.

42. (New) A method according to claim 26, wherein the security-relevant operations are key permutations or permutations of other secret data.

43. (New) A method according to claim 34, wherein the security-relevant operations are key permutations or permutations of other secret data.